Gaining Competitive Advantages in Cyberspace *through the Integration of Breakthrough Technologies in Autonomy, Artificial Intelligence, and Machine Learning*

Lieutenant Colonel Nathaniel D. Bastian, Ph.D.

ABSTRACT

Cyberspace has characteristics that differ from air, land, maritime, and space domains, which affect how the Joint Force operates and defends it. Fast-moving innovations are transforming the character of warfare in cyberspace, requiring novel technology integration. Effective integration of breakthrough technologies in autonomy, artificial intelligence, and machine learning into cyberspace can enable competitive advantages to be gained that enhance the combat power of joint forces conducting multi-domain operations. These technologies help shorten the sensor-to-shooter pathway to accelerate and optimize decision-making processes. These technologies also permit the enhancement of cyber situational understanding from the ingest, fusion, synthesis, analysis, and visualization of big data from varied cyber data sources to enable decisive, warfighting information advantage via the display of key cyber terrain with relevance in the commander's area of operations at the tactical edge. These technologies engender actionable information and recommendations to optimize human-machine decision-making via autonomous active cyber defense to effectively execute command and control while informing resourcing decisions. Competitive advantages gained allow key actions to be taken to generate, preserve, and apply informational power against a relevant actor while also permitting maneuver through the information environment.

INTRODUCTION AND BACKGROUND

Cyberspace has characteristics that differ from the air, land, maritime, and space domains. These characteristics affect how the Joint Force operates and defends cyberspace infrastructure, information, information systems, and data.[1] Joint forces have integrated and synchronized cyberspace capabilities along with the

LTC Nathaniel D. Bastian, Ph.D., is an Academy Professor at the United States Military Academy at West Point. He serves as Chief Data Scientist and Senior Research Scientist at the Army Cyber Institute (ACI) within the Department of Electrical Engineering and Computer Science, as well as Assistant Professor of Operations Research and Data Science with a dual faculty appointment in the Department of Systems Engineering and the Department of Mathematical Sciences. He leads the ACI's Data and Decision Sciences Division, directs the ACI's Intelligent Cyber-Systems and Analytics Research Lab and the ACI's Internet of Things Research Lab, and co-directs the ACI's Cyber Modeling and Simulation Research Lab. He has co-authored 80+ refereed publications, received $4M+ in externally-funded research monies from DEVCOM, NSA, AFRL, OUSD(R&E), DARPA, and NSF, served as a Visiting Research Fellow at the Johns Hopkins University Applied Physics Lab, and served as Distinguished Visiting Professor at the NSA.

authorities to conduct effective cyberspace operations as part of an overall combined arms strategy in support of Multi-Domain Operations (MDO) and Joint All-Domain Command and Control (JADC2). Cyberspace operations provide the commander the capability to process and manage operationally relevant actions, allowing simultaneous and linked maneuver, in, through and across multiple domains and the information environment, while engaging adversaries and populations directly across time, space, and scale.[2]

The information environment (IE) is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.[3] To manage the complexity of the cyberspace domain, the military divided it into separate layers, to include physical, logical, and cyber-persona.[4] Connections between the layers of cyberspace generate a portion of the IE that is divided into three dimensions – physical, informational, and cognitive; each dimension is associated with a specific layer of cyberspace[5] in which the latest technology can be integrated.

Fast-moving trends are rapidly transforming the character of warfare in cyberspace, which include significant advances in science and technology. These new discoveries and innovations are occurring at a breakneck pace. While the nature of war may remain constant, its speed, automation, effects, and increasingly integrated multi-domain conduct are changing, requiring novel technology integration. However, which breakthrough technologies and in what ways can their subsequent integration engender competitive advantage gains in cyberspace? Effective integration of breakthrough technologies in autonomy, artificial intelligence, and machine learning into cyberspace can enable competitive advantages to be gained to help provide joint commanders a full range of physical, virtual, lethal, and nonlethal capabilities tailored to enhance the combat power of joint forces conducting MDO. First, these technologies can help shorten the sensor-to-shooter pathway to accelerate and optimize decision-making composed of a complex sequence of operations to be performed in varied cyberspace environments and situations. Second, these technologies permit the enhancement of cyber situational understanding from the ingest, fusion, synthesis, analysis, and visualization of big data from varied cyber data sources to enable decisive, warfighting information advantage via the display of key terrain in cyberspace with relevance in the commander's area of operations at the tactical edge. Third, these technologies help engender actionable information and recommendations to optimize (accelerate, augment, and improve) human-machine decision-making via autonomous active cyber defense to effectively execute C2 while informing resourcing decisions.

To define these technologies, autonomy is the ability of a system to respond to situations by independently composing and selecting among different courses of action to accomplish goals based on knowledge and a contextual understanding of the world, itself, and the situation. Moreover, autonomy can best be expressed as a state of technological activity in which human interaction is limited or completely removed. Artificial intelligence (AI) is generally defined as a set of symbolic and/or non-symbolic techniques that enable machines to perform tasks that normally require human intelligence.[7] As a subset of AI, machine learning (ML) entails statistical/probabilistic algorithms that learn patterns in data as opposed to the use of symbolic representations of human knowledge.[8]

Shortened Sensor-to-Shooter Pathway for Accelerated and Optimized Decision-Making

One competitive advantage to be gained in cyberspace is that breakthrough autonomy AI, and ML technologies can help increase the automation of operational processes/functions and data processing while improving situational awareness.[9] The effective integration of these breakthrough technologies can enable the timely and optimized combination of software, sensors, systems, and humans to allow a complex sequence of operations to be performed in varied cyberspace environments and situations.[10] Currently, the Joint Force lacks a digitized network lethality backbone at scale, where warfighters must manually assess sensor data, identify targets, and then choose the weapon of choice to inform the commander's engagement decisions. Further, there is no digitized collaboration between platforms and C2 nodes, and there is no ability for commanders to leverage sensor data across the formation from multiple inputs to make informed, collaborative, and optimized decisions. Moreover, these sensor-to-human-to-shooter networks often have long processing times between target identification and target engagement, which has the potential to hinder successful execution of MDO significantly. Cyberspace infrastructure, however, is network-agnostic as it supports all users.[11] Cyberspace operations, in conjunction with autonomy, AI, and ML technology-enhanced cyberspace infrastructure, make it possible to shorten the sensor-to-shooter pathway to accelerate and optimize decision-making in terms of the best available shooter to respond with.

For example, the U.S. Army's Program Executive Officer for Intelligence, Electronic Warfare, and Sensors (PEO IEW&S) has the Tactical Intelligence Targeting Access Node (TITAN) modernization program within its Project Manager for Intelligence Systems & Analytics (PM IS&A) that is developing and integrating autonomy, AI, and ML technologies into cyberspace operations to automate target recognition, identification, and geolocation from multiple sensors to fuse the common intelligence picture and make target recommendations that reduce sensor-to-shooter timelines.[12] TITAN is a scalable and expeditionary intelligence ground station that supports commanders across the JADC2 battlefield framework with capabilities tailored to echelon. The capability ingests space and high altitude, aerial and terrestrial layer sensors and integrates an AI system, known as Prometheus,[13] to rapidly fuse and synthesize the sensor feeds into meaningful information to then provide target nominations directly to fires command and control networks as well as multi-discipline intelligence support to targeting and situational awareness in support of mission command.[14] Once targets are nominated, an AI-enabled targeting system known as FIRES Synchronization to Optimize Responses in Multi-Domain Operations (FIRESTORM), which is a science and technology effort led by the U.S. Army Combat Capabilities Development Command (DEVCOM) Armament Center, then ingests the sensor data (radio data link feeds, etc.) of adversary threats from Prometheus, uses One World Terrain to map the battlefield (navigational and terrain-specific, weather conditions, target coordinates, and precisely identified enemy location information), and optimally recommends the best weapon system to engage specific targets.[15]

In this example, the primary competitive advantage gained in cyberspace is saving the Joint Force commander's time for decision-making (reduced from 20 minutes to 32 seconds)[16] while providing actionable, effective, and efficient recommendations to deliver the right effects in near real time. Specifically, an integrated and scalable intelligence, surveillance, and reconnaissance (ISR) targeting and tasking capability shortens the sensor-to-shooter pathway by receiving multi-intelligence sensor feeds and directly down links them from strategic to tactical (process), uses on-board autonomy, AI and ML technologies to conduct target detection and mensuration to feed the intelligence common operating picture (exploit). This provides targetable data to decision-makers and fires C2 platforms for effect (disseminate), and finally uses an AI-enabled decision aid for weapon-target matching (optimize) to determine the best firing system to respond to the given threats (based on the terrain, available weapons, proximity, and number of other threats) while providing critical target deconfliction and an updated common operating picture (COP) for enemy and friendly situations.[17] Overall, the integration of breakthrough technologies leads to reduced target engagement time, accelerated and coordinated response of assets across multiple domains, faster determination of information relevant/important to the mission, and reduced decision cycle time and data overhead that enable success for Joint forces conducting MDO. Information-centric technologies, where network connections are ad hoc and information exchange and interconnectivity fluctuate at speeds beyond human capacity,[18] allow competitive advantages to be gained in cyberspace in the form of networked lethality. Knowledge, capabilities, and network-centric processing technologies that use autonomy, AI and ML seamlessly integrate networked sensors, target acquisition assets, effects assets, and warfighters to enable delivery of responsive and decisive effects on targets at all echelons.

*Enhanced Cyber Situational Understanding through Advances in Big Data Analytic*s

Another competitive advantage gained in cyberspace leverages advances in big data analytics to enhance cyber situational understanding by permitting the depiction, perception, and understanding of relevant cyberspace impacts that help enable the delivery of effects by tactical maneuver commanders in support of MDO. Many of these advances in big data analytics focus on ingesting, fusing, synthesizing, analyzing, and visualizing big data from varied cyber data sources that present significant volume, velocity, variety, veracity, and visualization issues.[19] Sample cyber data sources include host-based alerts, intrusion alerts, signature updates, vulnerability scans, network traffic (network flow, system logs, packet capture), network device status, security logs, powershell logs, and many more. Most of these advances in big data analytics stem from the research, development, and integration of breakthrough technologies in autonomy, AI and ML that use novel algorithms, methods, architectures, and computing mechanisms to ingest and tag massive data sets at the speed of cyber, to collect data with seemingly unbounded storage capacity with easy query and retrieval, to bring analytic tools to analysts at the tactical edge, and to rapidly generate visualizations that display key cyber terrain for improved decision-making while increasing operational efficiency.[20]

One advancement in big data analytics leverages a ML technology known as deep learning (DL), which is a subfield of ML that uses neural network algorithms with a sophisticated, multi-layer computational architecture to learn hierarchical representations of data. In a network intrusion detection system setting, for example, traditional ML techniques require the extraction of features from raw network traffic; typically, cyberspace subject matter experts analyze the network traffic and extract optimum features that are then used to train ML models useful to detect cyber-attacks. This approach, however, is resource-intensive, not scalable or generalizable across varied cyber data sources, and can result in information loss during data pre-processing.[21] Research scientists from the Army Cyber Institute (ACI) at West Point and the U.S. Army DEVCOM Army Research Laboratory (ARL) recently developed and applied a novel DL algorithm leveraging a one-dimensional convolutional neural network (1D-CNN) architecture that achieves an accuracy of 99% for network intrusion detection using only the bytes of the raw network traffic (i.e., packet capture data).[22] Follow-up research and development from the ACI/ARL team led to another advance in big data analytics known as transfer learning, which seeks to create DL models for a target domain that are pre-trained on some source domain (i.e., take information from one task and use it advantageously to learn a related task), to create and distribute the DL technology to tactical edge, computationally constrained environments.[23] They were able to conduct transfer learning successfully by transferring all main layers of the pre-trained 1D-CNN model combined with an edge retrained random forest ML model to obtain over 96% accuracy on the tactical network intrusion detection task with only 5,000 training samples on an AI-enabled edge device with an edge training time of only 67 seconds.[24] The ability to use such breakthrough DL technology to accurately and efficiently detect indicators of compromise at the tactical edge enables enhanced cyber situational understanding via integration of command post, cyberspace big data analytic tools that allow maneuver commanders and cyber defenders to depict and understand cyber terrain, make informed decisions, and remain effective and agile in MDO.

These advances in big data analytics that leverage breakthrough technologies in autonomy, AI and ML can be uniquely integrated across the Cyber Mission Force to immediately enhance cyber situational understanding and help gain competitive advantage in cyberspace. For instance, the U.S. Army's Program Executive Officer for Enterprise Information Systems (PEO EIS) has the Cyber Analytics and Detection (CAD) modernization program within its Project Manager for Defensive Cyber Operations (PM DCO) that aims to provide a "cyberspace analytics capability that offers interfaces and visualizations accessible by cyberspace defenders at all levels to facilitate counter-reconnaissance activities aimed at discovering the presence of advanced or sophisticated cyber threats and vulnerabilities."[25] The CAD program manages the Army's Big Data Platform (BDP), which is a data operating system used as the foundation for the cyber data fabric at Army Cyber Command (ARCYBER). ARCYBER's cloud-enhanced BDP, known as Gabriel Nimbus, is used at enterprise and strategic level operations, but they also have lighter versions of the BDP that are used at operational and tactical levels. Thus, the BDP's open-system architecture can easily integrate these advances in big data analytics to enhance cyber situational understanding[26] at the enterprise, strategic, operational, and tactical levels. Moreover, the U.S. Army's Program Executive Officer for Command Control Communications-Tactical (PEO C3T) has the Cyber Situational Understanding (Cyber SU) modernization program within its Project Manager for Mission Command Cyber (PM MC Cyber) that ingests data from PM DCO and other Army program offices to "enable visualization, analysis, and understanding of cyber and electromagnetic activities"[27] at the tactical edge. The Cyber SU product allows for integration of breakthrough technologies in autonomy, AI and ML that create advances in big data analytics to facilitate "informed planning, timely decision making, and mission accomplishment in the cyber-contested operating environment."[28] This enhanced cyber situational understanding allows direct gains in cyberspace competitive advantage such as network awareness (asset identification, vulnerability and incident management, etc.), threat awareness (adversary dispositions/actions, insider threat, etc.), and mission awareness (operational assessment, cyberspace mission impacts, etc.). Further, an AI-enhanced cyber situational understanding capability provides the ability to identify and display risk to system and equipment dependencies that have direct impact on combat missions when faced with a threat. Hence, these technologies are the pivot around which big data will be turned into actionable insight and knowledge and, ultimately, a decisive, warfighting information advantage needed to gain and maintain decision dominance.

Optimized Human-Machine Decision-Making via Autonomous Active Cyber Defense

A final competitive advantage gained in cyberspace is that these technologies can help realize autonomous active cyber defense that augments cyber defenders in their threat assessment and interpretation of vast amounts of cyber data to produce actionable information and recommendations to decision-makers to effectively execute C2 and inform optimal resource allocation decisions in terms of prioritization of incident response. Breakthrough technologies in autonomy, AI, and ML have the ability and capacity to make independent decisions and act upon these decisions rapidly, while at the same time, can work as part of a cyberspace operations team that includes humans.[29] Many of these technologies can collaborate with humans who will retain control and final decision-making authority while enhancing mission awareness of the cyber terrain and reducing the risk to personnel during operations. Thus, the integration of these technologies has the potential to impact the speed of the decision cycle decisively. Given that autonomous active cyber defense capabilities can detect, evaluate, and respond before a human operator alone can understand and react,[30] they should be used to optimize human-machine decision-making for the "collection of synchronized, real-time capabilities to discover, define, analyze, and mitigate cybers threats and vulnerabilities."[31] This includes technologies that learn and manage network topologies,[32] identify and manage trusted users, detect network anomalies, identify threats, and undertake mitigation and response action.[33]

As an example, the Joint Force Headquarters-Department of Defense Information Network (JFHQ-DODIN) has the mission to secure, operate, and defend the DODIN by integrating intelligence information, network operations, security actions, defensive cyberspace actions, and assessment and inspection results for informed decision-making.[34] The integration of breakthrough technologies in autonomy, AI, and ML can help optimize human-machine decision-making for threat-informed operational prioritization that allows JFHQ-DODIN leadership to optimally assess, track, report and align readiness of cyber terrain with assigned forces and prioritized essential tasks. Researchers from the University of South Florida in collaboration with the ACI recently developed a novel AI technology, known as Deep VULMAN, for optimizing the dynamic cyber vulnerability management process.[35] This technology can be directly leveraged by JFHQ-DODIN via its Network Operations Centers, Cyber Security Service Providers, Cyber Protection Teams, etc. for threat-informed resource allocation decision-making. Typically, these cyber defenders scan the network with a vulnerability scanner to find vulnerabilities reported in the National Vulnerability Database, and the generated vulnerability report contains the vulnerabilities found in the network along with attributes such as a common vulnerability exposure (CVE) code, host name, description, common vulnerability scoring system severity (CVSS) rating, and more. These forces then must assign resources to mitigate the vulnerability instances by taking actions such as applying patches, disabling services, etc. The Deep VULMAN AI-based technology overcomes limitations in current approaches to vulnerability management using advanced techniques for sequential decision-making under uncertainty, including deep reinforcement learning and integer programming, to autonomously recommend optimal, robust vulnerability triage and mitigation plans/policies.[36] This example of optimized human-machine decision-making via autonomous active cyber defense for dynamic cyber vulnerability management directly leads to gains in cyberspace competitive advantage in that the number of JFHQ-DODIN resources to be allocated over time is optimized and important vulnerabilities are identified and prioritized for mitigation, given the optimized allocation of resources. As such, these technologies uniquely provide the ability for cyber defenders to ensure mission continuity and success.[37]

Additional competitive advantages in cyberspace can be gained through improved interaction between human cyber operators and their tools. Breakthrough technologies in autonomy, AI, and ML can be integrated to improve cyber operators' ability to meet the increasing size, speed, and complexity of the cyber battlefield. Specifically, the Cyber Mission Force lacks validated, scalable capabilities to document and model cyber workflows and infer operator intent in real time; these capabilities are necessary to augment workflows effectively. Traditional methods to model workflow manually and elicit expert operator knowledge are often time/labor intensive, and they produce static workflow models of current practices and tactics, techniques, and procedures (TTPs); these can become obsolete as cyber-attacks and tools are constantly evolving. Automated techniques that integrate these breakthrough technologies can learn and log new workflows, which can then be incorporated on an ongoing basis into an adaptive decision support system for autonomous active cyber defense to keep pace in this domain. Without such methods, shallow and stale models of cyberspace operations impair operational, training, and technology development and acquisition decisions. Enormous opportunities exist to rapidly advance human-AI capabilities by adopting and automating digital methods and cyber analytics that can leverage high-granularity, human-computer interaction (HCI) data to augment the cognitive capabilities of cyber operators. To advance the state of the art and enable cyberspace decision-support capabilities, these breakthrough technologies can be integrated to capture cyber operator performance and workflows in complex information environments. Moreover, a cybernetic control signal (i.e., a virtuous feedback loop between human and machine) that leverages these HCI data streams along with integrated autonomy, AI, and ML technologies to improve the definition, resolution, and performance of the conjoined cyber operator system can be implemented for optimized human-machine decision-making. Cyberspace competitive advantages can be gained using these technologies to automate and accelerate aspects of knowledge elicitation and mature digital recording into an assistive automation capability to provide decision support to cyber operators with expert TTPs that is responsive to current workflows and situation. This broadly mitigates risks associated with the adoption of complex and unproven technologies.

CONCLUSIONS AND RECOMMENDATIONS

As highlighted above, the effective integration of breakthrough technologies in autonomy, AI, and ML into cyberspace support to operations in the IE gain competitive advantages across the cyberspace layers and respective IE dimensions. This allows actions to be taken by the commander to generate, preserve, and apply informational power toward a relevant actor while permitting maneuver through the IE.

Given that ongoing research and development in new breakthrough technologies is leading to major advancements at an exponential pace, how can the operational, science and technology, and acquisition and sustainment cyberspace communities actively identify and exploit the next technological innovations that come our way? This is where strategic, active partnerships among industry, academia, and government organizations must be established, maintained, and leveraged through a mission-focused, robust ecosystem of diverse cyberspace technology innovators focused on technology development, assessment and deployment. Industry organizations, including startups, large system integrators, global companies and more, represent a vital part of the ecosystem with now direct links to military organizations in which emerging requirements can be directly communicated so that new breakthrough technologies in autonomy, AI, and ML can be rapidly integrated and deployed more quickly. Academic organizations, including universities, research institutions, federally funded research and development centers (FFRDCs) and university-affiliated research centers (UARCs) within the ecosystem can learn about emerging cyberspace technology needs and challenges, enabling them to scale research efforts and build novel technology solutions through direct access to military-relevant use cases and problem sets. Finally, government entities within the ecosystem can establish airtight collaborations with these world-class innovative partners from industry and academia to remain knowledgeable about the latest innovations to exploit.

Although the character of warfare in cyberspace is rapidly transforming due to continued technological advances, the persistent and sustained identification, exploitation, and integration of new breakthrough technologies in autonomy, AI, and ML will continue to ensure competitive advantage gains in cyberspace across the Joint Force leading to success in conducting MDO.

NOTES

1. Joint Publication 3-12, U.S. Department of Defense, *Cyberspace Operations* (Washington, DC: United States Department of Defense, 2018), I-2.
2. Ibid., I-7.
3. Joint Publication 3-13.1, U.S. Department of Defense, *Information Operations* (Washington, DC: United States Department of Defense, 2012, incorporating change 1, 2014), I-1.
4. Joint Publication 3-12, U.S. Department of Defense, I-3.
5. Joint Publication 3-13.1, U.S. Department of Defense, I-2.
6. Alexander Kott, *Intelligent Autonomous Agents are Key to Cyber Defense of the Future Army Networks* (West Point, NY: *The Cyber Defense Review*, vol. 3, issue 3, 2018,57-70), 58.
7. Nathaniel Bastian, *Building the Army's Artificial Intelligence Workforce* (West Point, NY: The Cyber Defense Review, vol. 5, issue 2, 2020, 59-63), 59.
8. Fernando Maymí and Scott Lathrop, *AI in Cyberspace: Beyond the Hype (*West Point, NY: *The Cyber Defense Review*, vol. 3, issue 3, 2018, 71-81), 77.
9. TRADOC Pamphlet 525-8-6, Department of the Army, *The U.S. Army Concept for Cyberspace and Electronic Warfare Operations 2025-2040* (Fort Eustis, VA: U.S. Army Training and Doctrine Command, 2018), 19.
10. Alexander Kott, 63.
11. Joint Publication 3-12, U.S. Department of Defense, I-5.
12. Nathan Strout, "What the Army's TITAN Program Means to Multidomain Operations," *C4ISRNET,* June 9, 2020, https://www.c4isrnet.com/battlefield-tech/it-networks/2020/06/09/what-the-armys-titan-program-means-to-multi-domain-operations/.
13. Nathan Strout, "Inside the Army's Futuristic Test of its Battlefield Artificial Intelligence in the Desert," *C4ISRNET*, September 25, 2020, https://www.c4isrnet.com/artificial-intelligence/2020/09/25/the-army-just-conducted-a-massive-test-of-its-battlefield-artificial-intelligence-in-the-desert/.
14. Nathan Strout, "Army's TITAN Program."
15. George Seffers, "Soldiers and Commanders to Assess FIRESTORM AI Technology," *SIGNAL*, June 8, 2021, https://www.afcea.org/content/soldiers-and-commanders-assess-firestorm-ai-technology.
16. Ibid.
17. Nathan Strout, "Assess FIRESTORM AI Technology."
18. Marc Chalé and Nathaniel Bastian, "Generating Realistic Cyber Data for Training and Evaluating Machine Learning Classifiers for Network Intrusion Detection Systems" (*Expert Systems with Applications,* vol. 207, issue 117936, 2022, 1-18), 1.
19. Tariq Mahmood and Uzma Afzal, *Security Analytics: Big Data Analytics for Cybersecurity – A Review of Trends, Techniques and Tools* (2013 IEEE 2nd National Conference on Information Assurance, 2013, 129-134), 130-131.
20. Rudy Guyonneau and Arnaud Le Dez, "Artificial Intelligence in Digital Warfare: Introducing the Concept of the Cyberteammate" (West Point, NY: *The Cyber Defense Review,* vol. 4, issue 2, 2019, 103-115), 105-106.
21. Michael De Lucia, Paul Maxwell, Nathaniel Bastian, Ananthram Swami, Brian Jalaian, and Nandi Leslie, *Machine Learning for Raw Network Traffic Detection* (2021 SPIE AI and ML for MDO Applications III, vol. 11746, issue 117460V, 2021, 1-11), 1.
22. Ibid.
23. David Bierbrauer, Michael De Lucia, Krishna Reddy, Paul Maxwell, and Nathaniel Bastian, "Transfer Learning for Raw Network Traffic Detection" (*Expert Systems with Applications*, 1-10, Under Review), 3.
24. Ibid., 7-9.
25. PEO Enterprise Information Systems, "Cyber Analytics and Detection," https://www.eis.army.mil/programs/cad.
26. TRADOC Pamphlet 525-8-6, Department of the Army, 24.
27. PEO Command Control Communications-Tactical, "Mission Command Cyber," https://peoc3t.army.mil/mc/mcc.php.
28. Ibid.
29. Rudy Guyonneau and Arnaud Le Dez, 108-109.
30. Alexander Kott, 61-62.
31. TRADOC Pamphlet 525-8-6, Department of the Army, 25.

NOTES

32. Ibid.
33. Rudy Guyonneau and Arnaud Le Dez, 111.
34. Defense Information Systems Agency, "Director," https://www.disa.mil/about/our-leaders/director.
35. Soumyadeep Hore, Ankit Shah, and Nathaniel Bastian, *An Artificial Intelligence-Enabled Framework for Optimizing the Dynamic Cyber Vulnerability Management Process* (39th International Conference on Machine Learning, PMLR 162, 2022, 1-21), 1.
36. Ibid., 2.
37. TRADOC Pamphlet 525-8-6, Department of the Army, 25.